AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for the containment of network communication, comprising the steps of:

determining whether one or more usage-conditions are met;

intercepting a connection message[[,]]; and

conditionally sending, based on the one or more usage-conditions, the connection message [[sent]] from a client to a server over a communication-conduit.[[; and]]

~~determining whether one or more communication-conduit usage-conditions are met.~~

2. (Currently amended) The method of Claim 1, further comprising the step of forwarding the connection message to the server over the communication-conduit when the one or more usage-conditions are met.

3. (Original) The method of Claim 2, wherein the determining step comprises identifying a first network address of the server, a second network address of the client and a port number of the communication-conduit.

4. (Currently amended) The method of Claim 3, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address [[or]] of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

5. (Currently amended) The method of Claim 2, wherein the determining step comprises (a) obtaining a confirmation from a human, (b) determining whether the communication-conduit was used by the client prior to the client's sending the connection message, or (c) determining whether the client sent the connection message within an authorized time-window.

6. (Original) The method of Claim 2, wherein the determining step comprises obtaining a confirmation from a human, wherein the human (a) is associated with the client[[,]] or (b) has administrative privilege.

7. (Currently amended) The method of Claim 2, wherein the determining step comprises (a) determining whether the client used the communication-conduit at any time prior to the client's sending the connection message, (b) determining whether the client used the communication-conduit within a specific time–window prior to the client's sending the connection message, or (c) determining whether the client used the communication-conduit within a pre-determined context prior to the client's sending the connection message, wherein the pre-determined context comprises a TCP connection or a session.

8. (Original) The method of Claim 2, wherein the determining step comprises determining whether a configuration of the client comprises one or more pre-determined data.

9. (Currently amended) The method of Claim 2, wherein the determining step comprises determining whether a repository comprises one or more authorization data pertinent to the connection message.

10. (Original) The method of Claim 2, wherein the determining step comprises authorizing temporary usage of the communication-conduit, wherein the temporary usage expires unless administrative approval is obtained (a) within a pre-determined time-window, (b) before the client sends a pre-determined number of messages, or (c) before the client uses a pre-determined number of distinct contexts, wherein a context comprises a TCP connection or a session.

11. (Currently amended) The method of Claim 2, wherein the determining step comprises determining whether the connection message is sent within a pre-determined time-window.

12. (Original) The method of Claim 11, wherein the pre-determined time-window comprises one or more weekday peak usage hours.

13. (Currently amended) The method of Claim 1, further comprising the step of discarding the connection message when the one or more usage-conditions are not met.

14. (Original) The method of Claim 13, wherein the determining step comprises identifying a first network address of the client, a second network address of the server and a port number of the communication-conduit.

15. (Original) The method of Claim 1, further comprising the step of logging a result of the determining step.

16. (Original) The method of Claim 1, further comprising the step of notifying a system-administrator of a result of the determining step.

17. (Currently amended) A method for the containment of network communication, comprising the steps of:

determining whether one or more service-conditions are met;

intercepting a [[first]] service-initiation request[[,]]; and

conditionally sending, based on the one or more service-conditions, the service-initiation request [[sent]] from a client to a server over a network.[[; and]]

~~determining whether one or more service-conditions are met.~~

18. (Currently amended) The method of Claim 17, further comprising the step of forwarding the [[first]] service-initiation request to the server over the network when the one or more service-conditions are met.

19. (Original) The method of Claim 18, wherein the determining step comprises identifying a first network address of the server and a second network address of the client.

20. (Original) The method of Claim 19, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

21. (Currently amended) The method of Claim 18, wherein the determining step comprises (a) obtaining a confirmation from a human or (b) determining whether the client sent the [[first]] service-initiation request within an authorized time-window.

22. (Currently amended) The method of Claim 18, wherein the determining step comprises identifying a request-type indicated by the [[first]] service-initiation request.

23. (Currently amended) The method of Claim 18, wherein the determining step comprises determining whether a second service-initiation request of [[the]] a same request-type as the [[first]] service-initiation request (a) was forwarded to the server at any time prior to the client's sending the [[first]] service-initiation request (b) was forwarded to the server within a pre-determined time-window prior to the client's sending the [[first]] service-initiation request, or (c) was forwarded to the server within a specific context, wherein a context comprises a TCP connection or a session.

24. (Currently amended) The method of Claim 18, wherein the determining step comprises determining whether a second service-initiation request of the one or more pre-determined request-types (a) was forwarded to the server at any time prior to the client's sending the [[first]] service-initiation request, (b) was forwarded to the server within a pre-determined time-window prior to the client's sending the [[first]] service-initiation request, or (c) was forwarded to the server within a specific context, wherein a context comprises a TCP connection or a session.

25. (Currently amended) The method of Claim 17, further comprising the step of discarding the [[first]] service-initiation request when the one or more usage-conditions are not met.

26. (Currently amended) The method of Claim 25, wherein the determining step comprises identifying a first network address [[or]] of the client and a second network address of the server.

27. (Original) The method of Claim 17, further comprising the step of logging a result of the determining step.

28. (Original) The method of Claims 17, further comprising the step of notifying a system-administrator of a result of the determining step.

29. (Currently amended) A system for the containment of network communication, comprising:

a communication-proxy for intercepting a connection message from a client to a server over a communication-conduit;

wherein the communication-proxy ~~determines~~ is programmed to determine whether one or more ~~communication-conduit~~ usage-conditions are met, and wherein the communication-proxy (a) forwards the connection message to the server over the communication-conduit when the one or more usage-conditions are met, or (b) discards the connection message when the one or more usage-conditions are not met.

30. (Currently amended) The method of Claim 29, wherein the communication-proxy (a) obtains a confirmation from a human, (b) determines whether the communication-conduit was used by the client prior to the client's sending the connection message, or (c) determines whether the client sent the connection message within an authorized time-window.

31. (Original) The system of Claim 29, wherein the communication-proxy identifies a first network address of the server, a second network address of the client and a port number of the communication-conduit.

32. (Currently amended) The method of Claim 31, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

33. (Currently amended) The system of Claim 31, wherein the communication-proxy resides in a network element ~~such as a switch or a router~~, the network element in a communication path between the client and the server.

34. (Original) The system of Claim 31, wherein the communication-proxy and the client reside on the same host.

35. (Original) The system of Claim 31, wherein the communication-proxy and the server reside on the same host.

36. (Currently amended) A system for the containment of network communication, comprising:

a service-proxy for intercepting a service-initiation request from a client to a server over a network;

wherein the service-proxy ~~determines~~ is configured to determine whether one or more service-conditions are met, and wherein the service-proxy (a) forwards the service-initiation request to the server over the network when the one or more service-conditions are met[[,]] or (b) discards the service-initiation request when the one or more service-conditions are not met.

37. (Currently amended) The system of Claim 36, wherein the service-proxy (a) obtains a confirmation of the one or more service-conditions being met from a human[[,]] or (b) ~~determines~~ is programmed to determine whether the client set the service-initiation request within an authorized time-window.

38. (Original) The system of Claim 36, wherein the service-proxy identifies a first network address of the server and a second network address of the client.

39. (Currently amended) The method of Claim 38, further comprising the step of sending a plurality of DHCP reply messages for binding a first address of a first host to a second address of a second host, the plurality of DHCP reply messages sent to a third host, the server residing on the first host, and the client residing on the third host.

40. (Currently amended) The system of Claim 38, wherein the service-proxy resides in a network element ~~such as a switch or a router~~, the network element in a communication path between the client and the server.

41. (Original) The system of Claim 38, wherein the service-proxy and the client reside on the same host.

42. (Original) The system of Claim 38, wherein the service-proxy and the server reside on the same host.

43. (Currently amended) The method of Claim 36, wherein the service-proxy determines a request-type indicated by the service-initiation request.